PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

scrambling order operations des

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **scrambling order operations des**

Found **84,577** of **173,942**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200

Best 200 shown

Result page: **1** 2 3 4 5 6 7 8 9 10 next

Relevance scale

1 A fast MPEG video encryption algorithm

Changgui Shi, Bharat Bhargava

September 1998 **Proceedings of the sixth ACM international conference on Multimedia**

**Publisher:** ACM Press

Full text available: pdf(805.58 KB) Additional Information: full citation, references, citings, index terms

**Keywords:** DES, MPEG codec, MPEG video encryption, multimedia data security

2 Performance analysis of MD5

Joseph D. Touch

October 1995 **ACM SIGCOMM Computer Communication Review , Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication SIGCOMM '95**, Volume 25 Issue 4

**Publisher:** ACM Press

Full text available: pdf(1.04 MB) Additional Information: full citation, abstract, references, citings, index terms

MD5 is an authentication algorithm proposed as the required implementation of the authentication option in IPv6. This paper presents an analysis of the speed at which MD5 can be implemented in software and hardware, and discusses whether its use interferes with high bandwidth networking. The analysis indicates that MD5 software currently runs at 85 Mbps on a 190 Mhz RISC architecture, a rate that cannot be improved more than 20-40%. Because MD5 processes the entire body of a packet, this data ra ...

3 Efficient frequency domain video scrambling for content access control

Wenjun Zeng, Shawmin Lei

October 1999 **Proceedings of the seventh ACM international conference on Multimedia (Part 1)**

**Publisher:** ACM Press

Full text available: pdf(1.65 MB) Additional Information: full citation, abstract, references, index terms

Multimedia data security is very important for multimedia commerce on the Internet such as video-on-demand and real-time video multicast. Traditional cryptographic algorithms for data security are often not fast enough to process the vast amount of data generated by the multimedia applications to meet the real-time constraints. This paper presents a joint encryption and compression framework in which video data are scrambled efficiently in the frequency domain by employing selective bit scr ...

**Keywords**: compression, content access control, multimedia commerce, multimedia encryption, multimedia security, selective encryption, video scrambling

4 Papers: Context-agile encryption for high speed communication networks

Lyndon G. Pierson, Edward L. Witzke, Mark O. Bean, Gerry J. Trombley
January 1999 **ACM SIGCOMM Computer Communication Review**, Volume 29 Issue 1
**Publisher:** ACM Press
Full text available: pdf(1.43 MB) Additional Information: full citation, abstract, references

Different applications have different security requirements for data privacy, data integrity, and authentication. Encryption is one technique that addresses these requirements. Encryption hardware, designed for use in high-speed communications networks, can satisfy a wide variety of security requirements if the hardware implementation is key-agile, key length-agile, mode-agile, and algorithm-agile. Hence, context-agile encryption provides enhanced solutions to the secrecy, interoperability, and ...

5 New directions for integrated circuit cards operating systems

Pierre Paradinas, Jean-Jacques Vandewalle
January 1995 **ACM SIGOPS Operating Systems Review**, Volume 29 Issue 1
**Publisher:** ACM Press
Full text available: pdf(422.64 KB) Additional Information: full citation, abstract, index terms

Integrated circuit cards or smart cards are now well-known. Applications such as electronic purses (cash units stored in cards), subscriber identification cards used in cellular telephone or access keys for pay-TV and information highways emerge in many places with millions of users. More services are required by applications providers and card holders. Mainly, new integrated circuit cards evolve towards non-predefined multi-purpose, open and multi-user applications. Today, operating systems imp ...

**Keywords**: integrated circuit card applications, integrated circuit card operating system, object-oriented technologies, secured method execution

6 Session 1: Applications: New directions for integrated circuit cards operating systems

Pierre Paradinas, Jean-Jacques Vandewalle
September 1994 **Proceedings of the 6th workshop on ACM SIGOPS European workshop: Matching operating systems to application needs**
**Publisher:** ACM Press
Full text available: pdf(437.96 KB) Additional Information: full citation, abstract, references

Integrated circuit cards or smart cards are now well-known. Applications such as electronic purses (cash units stored in cards), subscriber identification cards used in cellular telephone or access keys for pay-TV and information highways emerge in many places with millions of users. More services are required by applications providers and card holders. Mainly, new integrated circuit cards evolve towards non-predefined multi-purpose, open and multi-user applications. Today, operating systems imp ...

**Keywords**: Integrated Circuit Card Applications, Integrated Circuit Card Operating System, Object-Oriented Technologies, Secured method execution

7 Special session on reconfigurable computing: Adaptive architectures for an OTN processor: reducing design costs through reconfigurability and multiprocessing

Tudor Murgan, Mihail Petrov, Mateusz Majer, Peter Zipf, Manfred Glesner, Ulrich Heinkel, Joerg Pleickhardt, Bernd Bleisteiner
April 2004 **Proceedings of the 1st conference on Computing frontiers**
**Publisher:** ACM Press
Full text available: pdf(1.01 MB) Additional Information: full citation, abstract, references, citings, index terms

The standardisation process of Optical Transport Networks generally spans a long period of time. For providers intending to be present early on the market, this implies costly design re-spins if the wrong "flavour" of the protocol standard has been implemented. Extending a protocol processing device through application specific reconfigurable elements or multiprocessor units augment its flexibility. Thus, the architecture can be upgraded to standard updates or changes not even considered at desi ...

**Keywords**: ITU-T G.709, multiprocessor and reconfigurable architectures, optical transport networks, standard upgrades

8 Power Attack Resistant Cryptosystem Design: A Dynamic Voltage and Frequency Switching Approach
Shengqi Yang, Wayne Wolf, N. Vijaykrishnan, D. N. Serpanos, Yuan Xie
March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 3 DATE '05**
**Publisher:** IEEE Computer Society
Full text available: pdf(291.83 KB) Additional Information: full citation, abstract

A novel power attack resistant cryptosystem is presented in this paper. Security in digital computing and communication is becoming increasingly important. Design techniques that can protect cryptosystems from leaking information have been studied by several groups. Power attacks, which infer program behavior from observing power supply current into a processor core, are important forms of attacks. Various methods have been proposed to countermeasure the popular and efficient power attacks. Howe ...

9 Cryptographic technology: fifteen year forecast
Whitfield Diffie
September 1982 **ACM SIGACT News**, Volume 14 Issue 4
**Publisher:** ACM Press
Full text available: pdf(1.30 MB) Additional Information: full citation, abstract, references

This paper examines the forces driving public development of cryptography today and projects the course of the field over the next fifteen years with attention to the possible influence of government regulation.This paper was prepared, under contractual arrangements to CRC Systems, in support of the Commerce Department (National Telecommunications and Information Administration, Special Projects Office) response to a White House Office of Science and Technology Policy request that the secretarie ...

10 Session: Chinese numbers, MIX, scrambling, and range concatenation grammars
Pierre Boullier
June 1999 **Proceedings of the ninth conference on European chapter of the Association for Computational Linguistics**
**Publisher:** Association for Computational Linguistics
Full text available: pdf(747.58 KB) Publisher Site Additional Information: full citation, abstract, references

The notion of mild context-sensitivity was formulated in an attempt to express the formal power which is both necessary and sufficient to define the syntax of natural languages. However, some linguistic phenomena such as Chinese numbers and German word scrambling lie beyond the realm of mildly context-sensitive formalisms. On the other hand, the class of range concatenation grammars provides added power w.r.t. mildly context-sensitive grammars while keeping a polynomial parse time behavior. In t ...

11 Methods for encrypting and decrypting MPEG video data efficiently
Lei Tang
February 1997 **Proceedings of the fourth ACM international conference on Multimedia**
**Publisher:** ACM Press
Full text available: pdf(1.45 MB) Additional Information: full citation, references, citings, index terms

**Keywords:** MPEG codec, compression, multimedia commerce, multimedia encryption, multimedia security

12 Session 2: Review and analysis of synthetic diversity for breaking monocultures
James E. Just, Mark Cornwell
October 2004 **Proceedings of the 2004 ACM workshop on Rapid malcode**
**Publisher:** ACM Press
Full text available: pdf(356.14 KB) Additional Information: full citation, abstract, references, index terms

The increasing monoculture in operating systems and key applications and the enormous expense of N-version programming for custom applications mean that lack of diversity is a fundamental barrier to achieving survivability even for high value systems that can afford hot spares. This monoculture makes flash worms possible. Our analysis of vulnerabilities and exploits identifies key assumptions required to develop successful attacks. We review the literature on synthetic diversity techniques, f ...

**Keywords:** diversity, n-version programming, vulnerability

13 Data base directions: the next steps
John L. Berg
November 1976 **ACM SIGMOD Record , ACM SIGMIS Database**, Volume 8 , 8 Issue 4 , 2
**Publisher:** ACM Press
Full text available: pdf(9.95 MB) Additional Information: full citation, abstract

What information about data base technology does a manager need to make prudent decisions about using this new technology? To provide this information the National Bureau of Standards and the Association for Computing Machinery established a workshop of approximately 80 experts in five major subject areas. The five subject areas were auditing, evolving technology, government regulations, standards, and user experience. Each area prepared a report contained in these proceedings. The proceedings p ...

**Keywords:** DBMS, auditing, cost/benefit analysis, data base, data base management, government regulation, management objectives, privacy, security, standards, technology assessment, user experience

14 The design and implementation of a private message service for mobile computers
David A. Cooper, Kenneth P. Birman
August 1995 **Wireless Networks**, Volume 1 Issue 3
**Publisher:** Kluwer Academic Publishers
Full text available: pdf(1.35 MB) Additional Information: full citation, abstract, references

Even as wireless networks create the potential for access to information from mobile platforms, they pose a problem for privacy. In order to retrieve messages, users must periodically poll the network. The information that the user must give to the network could potentially be used to track that user. However, the movements of the user can also be used to hide the user's location if the protocols for sending and retrieving messages are carefully designed. We have developed a replicated memo ...

15 The FINITE STRING newsletter: Abstracts of current literature
Computational Linguistics Staff
July 1986 **Computational Linguistics**, Volume 12 Issue 3
**Publisher:** MIT Press
Full text available: pdf(2.25 MB) Publisher Site
Additional Information: full citation

16 Data Security
Dorothy E. Denning, Peter J. Denning
September 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 3
**Publisher:** ACM Press
Full text available: pdf(1.97 MB) Additional Information: full citation, references, citings, index terms

17 Power modeling and optimization for embedded systems: Energy-efficient data scrambling on memory-processor interfaces
Luca Benini, Angelo Galati, Alberto Macii, Enrico Macii, Massimo Poncino
August 2003 **Proceedings of the 2003 international symposium on Low power electronics and design**
**Publisher:** ACM Press
Full text available: pdf(147.39 KB) Additional Information: full citation, abstract, references, index terms

Crypto-processors are prone to security attacks based on the observation of their power consumption profile. We propose new techniques for increasing the non-determinism of such profile, which rely on the idea of introducing randomness in the bus data transfers. This is achieved by combining data scrambling with energy-efficient bus encoding, thus providing high information protection at no energy cost.Results on a set of bus traces originated by real-life applications demonstrate the applicabil ...

**Keywords:** bus encoding, data scrambling, power attacks

18 Applications: Isolating cross-linguistic parsing complexity with a principles-and-parameters parser: a case study of Japanese and English
Sandiway Fong, Robert C. Berwick
August 1992 **Proceedings of the 14th conference on Computational linguistics - Volume 2**
**Publisher:** Association for Computational Linguistics
Full text available: pdf(583.76 KB) Additional Information: full citation, references

19 Information theoretic implications for pairing heaps
Michael L. Fredman
May 1998 **Proceedings of the thirtieth annual ACM symposium on Theory of**

**computing**
**Publisher:** ACM Press
Full text available: pdf(1.19 MB) Additional Information: full citation, references, index terms

20 A Self Managing Secondary Memory system
Manlio DeMartinis, G. Jack Lipovski, Stanley Y.W. Su, J. K. Watson
January 1976 **ACM SIGARCH Computer Architecture News , Proceedings of the 3rd annual symposium on Computer architecture ISCA '76**, Volume 4 Issue 4
**Publisher:** ACM Press
Full text available: pdf(909.18 KB) Additional Information: full citation, abstract, references, citings, index terms

A Self Managing Secondary Memory (SMSM) organization is proposed herein, in which hardware directly assists the storage, retrieval and management of arbitrary length records on such devices as fixed head discs or charge coupled devices (CCD's). This paper emphasizes some of the techniques used to implement an SMSM system. In an SMSM, fixed length words are organized into variable length records, and these records are packed into a file. The first word of the record, a label, can ...

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2006 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player